EXPRESS MAIL NO. EV301024491US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Cheh GOH, et al.	)	
Serial No.: Not yet assigned	)	
Filed: Concurrently herewith	)	Our Ref: B-5236 621255-8
For: "DATA OUTPUT METHOD, SYSTEM AND APPARATUS"	)	Date: September 16, 2003

CLAIM TO PRIORITY UNDER 35 U.S.C. 119

MAIL STOP PATENT APPLICATION
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

[X] Applicants hereby make a right of priority claim under 35 U.S.C. 119 for the benefit of the filing date(s) of the following corresponding foreign application(s):

COUNTRY	FILING DATE	SERIAL NUMBER
Great Britain	17 September 2002	0221639.8

[ ] A certified copy of each of the above-noted patent applications was filed with the Parent Application No._____.

[X] To support applicants' claim, a certified copy of the above-identified foreign patent application is enclosed herewith.

[ ] The priority document will be forwarded to the Patent Office when required or prior to issuance.

Respectfully submitted,

Richard P. Berg
Attorney for Applicant
Reg. No. 28,145

LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, CA 90036
Telephone: (323) 934-2300
Telefax: (323) 934-0202

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 14 November 2002

Patents Form 1/77

Patents Act 1977
(F 16)

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — 300110535-1 GB

17 SEP 2002

2. Patent application number *(The* 0221639.8

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304, USA

Patents ADP number *(if you know it)*

Delaware, USA 4965886001

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention — Method and apparatus for printing

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Chris Harrison
Hewlett-Packard Ltd, IP Section
Filton Road, Stoke Gifford
Bristol BS34 8QZ

8191143901

Patents ADP number *(if you know it)*

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	15
Claim(s)	4
Abstract	1
Drawing(s)	2+2

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	1 ✓
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	1 ✓
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	Fee Sheet ✓

11. I/We request the grant of a patent on the basis of this application.

Signature  Date 16/9/2002

12. Name and daytime telephone number of person to contact in the United Kingdom: Tony Judd Tel: 0117-312-8026

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

METHOD AND APPARATUS FOR PRINTING

The present invention relates to a method, system and apparatus for printing.

A number of different techniques have been developed to minimise unauthorised access to data held on a computer apparatus or to data transmitted between computer apparatuses.

However, should a user print confidential information to a remote printer this can result in the confidential information being accessible to anyone who has access to the printer, which for mobile users can be particularly undesirable.

One solution to this problem has been to use a printer spooler, within a printer server, which will only deliver a job to a printer, for printing, if the recipients of the job authenticate themselves to the printer spooler.

However, this requires specific configuration of a printer spooler, which as a result can limit the conditions under which a document can be printed.

It is desirable to improve this situation.

In accordance with a first aspect of the present invention there is provided a computer system comprising a first computer entity for deriving an encryption key using a first data set that defines at least one policy for allowing the printing of a second data set and encrypting the second data set with the encryption key; and communication means for providing the encrypted second data set to a printer; wherein a second computer entity is arranged, on satisfaction of the at least one policy, to generate an associated decryption key to allow the printer to decrypt the encrypted second data set.

In accordance with a second aspect of the present invention there is provided a computer system comprising a first computer entity for deriving an encryption key using a first data set that defines at least one policy for allowing the printing of a second data set and encrypting the second data set with the encryption key; and communication means for providing the encrypted second data set to a printer; wherein a second computer entity is arranged, on satisfaction of the at least one policy, to issue an associated decryption key to allow the printer to decrypt the encrypted second data set.

Preferably the communication means provides the at least one policy to the second computer entity.

Preferably the second computer entity issues the at least one policy to the first computer entity.

Preferably the second computer entity is associated with a trusted authority.

Preferably the encryption key is derived with the first data set and a public parameter associated with the trusted authority.

Suitably the second data set is encrypted with the encryption key using a bilinear pairing or quadratic residue technique.

In accordance with a third aspect of the present invention there is provided a computer system comprising a first computer entity arranged to generate an encryption key using a first data set that defines a first policy for allowing the printing of a fifth data set in conjunction with a second data set that represents a first trusted party's public key and a third data set that defines a second policy for allowing the printing of the fifth data set in conjunction with a fourth data set that represents a second trusted party's public key, and encrypting the fifth data set with the encryption key; and communication means for

providing the encrypted fifth data set to a printer; wherein a second computer entity associated with the first trusted party is arranged, on satisfaction of the first policy, to issue an associated first decryption key and a third computer entity associated with the second trusted party is arranged, on satisfaction of the second policy, to issue an associated second decryption key, thereby allowing the printer to decrypt the encrypted fifth data set.

In accordance with a fourth aspect of the present invention there is provided a method for printing comprising deriving an encryption key using a first data set that defines at least one policy for allowing the printing of a second data set; encrypting the second data set with the encryption key; providing the encrypted second data set to a printer; arranging a first party to issue, on satisfaction of the at least one policy, an associated decryption key to allow decryption of the encrypted second data set, thereby allowing the printing of the second data set.

In accordance with a fifth aspect of the present invention there is provided a method for printing comprising generating a first data set that represents a first trusted party's public key; generating a second data set that represents a second trusted party's public key; generating an encryption key using a third data set that defines a first policy for allowing the printing of a fourth data set in conjunction with the first data set and a fifth data set that defines a second policy for allowing the printing of the fourth data set in conjunction with the second data set, and encrypting the fourth data set with the encryption key; and providing the encrypted fourth data set to a printer; providing an associated first decryption key to the printer generated by the first trusted party, on satisfaction of the first policy, and providing an associated second decryption key to the printer generated by the second trusted party, on satisfaction of the second policy, to allow decryption of the encrypted fourth data set.

In accordance with a sixth aspect of the present invention there is provided a printer comprising a receiver arranged to receive a first data set encrypted using a second data set, wherein the second data set defines at least one policy for allowing the printing of the first data set.

Preferably the receiver is arranged to receive an associated decryption key generated by a trusted authority on satisfaction of the at least one policy, thereby allowing printing of the first data set.

Suitably the trusted authority is incorporated within the printer in the form of a computer entity.

Preferably the printer further comprising a transmitter arranged to provide that at least one policy to a computer entity.

For a better understanding of the present invention and to understand how the same may be brought into effect reference will now be made, by way of example only, to the accompanying drawings, in which:-

Figure 1 illustrates a computer system according to a first embodiment of the present invention;

Figure 2 illustrates a computer system according to a second embodiment of the present invention;

Figure 3 illustrates a computer system according to a third embodiment of the present invention.

The present embodiment provides a printer that is arranged, using identifier based encryption as described below, to enforce policies and/or verification constraints associated with a job to be printed by the printer, where the job is sent to the printer, for printing, after being encrypted using an identifier based

encryption public key that is derived using the relevant policies and/or verification constraints.

Figure 1 shows a first computer entity 10, a second computer entity 20 and a printer 30 connected via a network 40, for example the Internet.

The first computer entity 10 represents a user 50 and the second computer entity 20 represents a trust authority 60.

The first and second computer entities 10, 20, are conventional computing devices as are well known to a person skilled in the art.

The first computer entity 10 includes a processor 70 that is arranged to allow the generation of policy and/or verification constraints that stipulate the requirements for allowing the printing of a document, for example a policy/verification constraint could stipulate that a document may only be printed at a specific printer. The policy and/or verification constraints can be expressed in any suitable form, for example XML format.

Additionally or alternatively, however, the first computer entity 10 could receiving policy and/or verification constraints for allowing the printing of a document, for example from the trust authority 60, via the network 40.

Once the policy and/or verification constraints have been generated, or received, by the first computer entity 10 the processor 70 is arranged to derive an encryption key using the policy and/or verification constraints and encrypts the document with the encryption key, as described below.

Once the document has been encrypted the document is forwarded, via the network 40, to the printer 30. Typically, if the policy and/or verification constraints have been generated by the user 50 a representation of the policy

and/or verification constraints are also forwarded to the printer 30 with the encrypted document.

The printer 30 includes an interface 80 for coupling the printer 30 to the network 40 and a processor 90.

Associated with the printer 30 is local printer information that includes device identity, serial number, location, etc.

On receipt of the encrypted document by the printer 30 the processor 90 is arranged, via the interface 80 and network 40, to contact the trust authority 60 to request an associated decryption key to allow the printer 30 to decrypt the received encrypted document. Additionally, the processor 90 is arranged, on receipt of associated policy and/or verification constraints, to forward the policy and/or verification constraints to the trust authority 60.

On receipt, by the trust authority 60, of a request from the printer 30 for a decryption key the trust authority 60 determines if the trust authority 60 has the associated policy and/or verification constraints used to derive the encryption key. The trust authority 60 will typically receive the policy and/or verification constraints via the printer 30, as described above, however other mechanisms could be established, for example the user 50 could provide the policy and/or verification constraints to the trust authority 60 directly. Alternatively, the trust authority 60 could generate the relevant policy and/or verification constraints and provide these to the user 50 to allow the user 50 to encrypt the document, as described below.

On receipt of the request for a decryption key with the relevant policy and/or verification constraints the trust authority 60 determines whether the appropriate policy and/or verification constraints have been complied with. If the trust authority 60 believes that the policy and/or verification constraints have been complied with the trust authority 60 generates an associated

decryption key and forwards the decryption key to the printer 30 to decrypt the document, as described below.

An embodiment of identifier based encryption using a bilinear map, such as Tate pairing and Weil pairing, to enable a document to be encrypted and decrypted will now be described, however other types of identifier based encryption may also be used, for example using quadratic residue technique.

For the purposes of this embodiment we use a modified Weil pairing with *G1* and *G2* denote two groups of prime order q in which the discrete logarithm problem is believed to be hard and for which there exists a computable bilinear map.

i.e. $e : G_1 \times G_1 \longrightarrow G_2$

G_1 is a group of points on an elliptic curve and G_2 is a subgroup of a multiplicative group of a finite field.

As the mapping between G_1 and G_2 is bilinear exponents/multipliers can be moved around. For example if $a, b, c \in \mathbb{F}_q$ and $P, Q \in G_1$ then

$$e(aP, bQ)^c = e(aP, cQ)^b = e(bP, cQ)^a = e(bP, aQ)^c = e(cP, aQ)^b = e(cP, bQ)^a$$
$$= e(abP, Q)^c = e(abP, cQ) = e(P, abQ)^c = e(cP, abQ)$$
$$= \ldots$$
$$= e(abcP, Q) = e(P, abcQ) = e(P, Q)^{abc}$$

To set up the system, choose a large (at least 512-bits) prime p such that $p = 2 \bmod 3$ and $p = 6q - 1$ for some prime $q > 3$, define an elliptic curve, E, as y^2

$= x^3 + 1$ over $\mathbb{F}_p$, and further, choose an arbitrary point, P, on E, i.e., $P \in E/\mathbb{F}_p$ of order q.

Additionally, for the purposes of this embodiment the following cryptographic hash functions are defined:

$H_1: \{0,1\}^* \rightarrow \mathbb{F}_p$;
$H_2: \mathbb{F}_{p^2} \rightarrow \{0,1\}^k$ for some security parameter k;
$H_3: \{0,1\}^k \times \{0,1\}^k \rightarrow \mathbb{Z}^*_q$,
$H_4: \{0,1\}^k \rightarrow \{0,1\}^k$.

A public/private key pair is defined for the trust authority 60 where the public key R is: $R \in$ G1 and the private key s is: $s \in \mathbb{F}_q$ with $R=sP \in G_1$.

Additionally, an identifier based public key Q_{ID} / private key S_{ID} pair is defined where the Q_{ID}, $S_{ID} \in G_1$ where the trust authority's public/private key pair (R,s) is linked with the identifier based public/private key by

$$S_{ID} = sQ_{ID} \text{ and } Q_{ID} = \text{MapToPoint } (H_1 (\text{ID}))$$

where ID is an identifier string.

Given a hash function $H_1: \{0,1\}^* \rightarrow \mathbb{F}_p$, algorithm MapToPoint works as follows on input $H_1(\text{ID}) = y_0 \in \mathbb{F}_p$:

(1) Compute $x_0 = (y_0^2 - 1)^{1/3} = (y_0^2 - 1)^{(2p-1)/3} \in \mathbb{F}_p$.

(2) Let $Q = (x_0, y_0) \in E/\mathbb{F}_p$ and set $Q_{ID} = 6Q \in G_1$.

(3) Output MapToPoint$(y_0) = Q_{ID}$.

As such identifier based encryption allows the holder of the private key S_{ID} of an identifier based key pair to decrypt a document sent to them encrypted using the associated public key Q_{ID} .

Consequently, the user 50 can derive a public key, Q_{print}, for the printer 30 using the policy and/or verification constraints as the identifier.

Once a public key has been derived the document, m, to be printed can be encrypted by performing the following computation.

- Selects a random number $\sigma \in \{0,1\}^k$.
- Computes $r = H_3(\sigma, m)$, where r is a random element that ensures only someone with the appropriate private key can decrypt the document, m.
- Computes $U = rP$.
- Computes $g_{ID} = \hat{e}(Q_{print}, R) \in \mathbb{F}_{p^2}$.
- Computes $V = \sigma \oplus H_2(g_{ID}{}^r)$.
- Computes $W = m \oplus H_4(\sigma)$.
- Sets the ciphertext to be $C = (U, V, W)$.

As stated above the ciphertext, which corresponds to the encrypted message, m, is forwarded to the printer 30.

The printer 30 registers with the trust authority 60 to obtain an associated private key for the printer's public key, where, as described above, the printer's public key is a representation of the policy and/or verification constraints, where the public key $H_1(\text{Printer}) = Q_{\text{Printer}}$ would map to a point on an elliptic curve defined by G_1.

On registration, the trust authority 60 provides the user 50 with the appropriate private key on confirmation that the policy and/or verification constraints have been complied with. The appropriate private key would be a

combination of the printer's public key and the trust authority's private key i.e. $S_{printer}=rQ_{printer}$.

On receipt of the private key the document is decrypted by performing the following computation:

- Tests $U \in E/\mathbb{F}_p$ of order q;
- Computes $x = \hat{e}(S_{print}, U)$;
- Computes $\sigma = V \oplus H_2(x)$;
- Computes $m = W \oplus H_4(\sigma)$;
- Computes $r = H_3(\sigma, m)$;
- Checks $U = rP$.

The above embodiment can be further expanded to include multiple trust authorities where the decryption key comprises component elements from the individual trust authorities. One embodiment of multiple trust authorities is shown in figure 2, which is based upon the computer system shown in figure 1 with the addition of a third computer entity 100, where the third computer entity 100 acts as a second trust authority 200, independent of the first trust authority 60.

As with the first trust authority 60 the second trust authority 200 has a unique public/private key pair.

As described below, the printer 30 has an independent identity (i.e. has independent policy and/or verification constraints with respect to the printing of a document) associated with each trust authority 60, 200, where each independent identity corresponds to a public key of the printer 30. Each trust authority 60, 200 generates a private key corresponding to the respective printer's public key, as described above. To send an encrypted document to the printer 30 the user 50 encrypts the document with a combination of the

printer's public keys associated with the respective trust authorities 60, 200 (i.e. the user's policy and/or verification constraints associated with the respective trust authorities) and the respective trust authority's public key. On receipt of the encrypted document the printer 30 decrypts the document with a combination of the trust authority's public keys and the private keys associated with the respective policy and/or verification constraints, where the printer 30 obtains the respective private keys from the respective trust authorities 60, 200 on compliance with the respective policy and/or verification constraints.

By way of illustration the following embodiment utilises identifier-based cryptography using Tate pairings to allow the generation of a public key that is a combination of independent identities (i.e. policy and/or verification constraints) associated with respective trust authorities 60, 200.

The first trust authority 60 has a public key R_1 and a corresponding private key s_1 where $R_1 = s_1P$, with P being a point on an elliptic curve, as described above.

The second trust authority 200 has a public key R_2 and a corresponding private key s_2 where $R_2 = s_2P$, with P being a point on an elliptic curve, as described above.

The user 50 defines a first and second set of policy and/or verification constraints that are associated with the first and second trust authorities 60, 200 respectively, that is to say with the first trust authority 60 the user 50 has an first set of policy and/or verification constraints ID1, with second trust authority 200 the user 50 had another set of policy and/or verification constraints ID2.

Accordingly, the user 50 has independent identity based private keys and public keys with each trust authority 60, 200, where the user's identity based

public key with the first trust authority 60 is $Q_{ID1} = H_1(ID1)$ and the user's identity based private key with the first trust authority 60 is S_{ID1}, where $S_{ID1} = s_1 Q_{ID1}$ and the user's identity based public key with the second trust authority 200 is $Q_{ID2} = H_1(ID2)$ and the user's identity based private key with the second trust authority 200 is S_{ID2}, where $S_{ID2} = s_2 Q_{ID2}$.

The user 50 encrypts a document m for sending to the printer by generating ciphertext V and W, where:

- Computes a MapToPoint $(H_1(ID_i)) = Q_{IDi}$ $(i = 1, \ldots, n) \in E/\mathbb{F}_p$ of order q.
- Selects a random number $\sigma \in \{0,1\}^k$.
- Computes $r = H_3(\sigma, m)$.
- Computes $U = rP$.
- Computes $g_{ID} = \Pi_{(1 \le i \le 2)} \hat{e}(Q_{IDi}, R_i) \in \mathbb{F}_{p^2}$.
- Computes $V = \sigma \oplus H_2(g_{ID'})$.
- Computes $W = m \oplus H_4(\sigma)$.
- Sets the ciphertext to be $C = (U, V, W)$.

Decryption is performed by the printer by computing:

- Tests $U \in E/\mathbb{F}_p$ of order q;
- Computes $x = \hat{e}(\Sigma_{(1 \le i \le 2)} S_{IDi}, U)$;
- Computes $\sigma = V \oplus H_2(x)$;
- Computes $m = W \oplus H_4(\sigma)$;
- Computes $r = H_3(\sigma, m)$;
- Checks $U = rP$.

where the respective identity based private keys are provided to the printer 30 on satisfactory compliance of the respective policy and/or verification constraints.

Accordingly, message m can only be decrypted with knowledge of both private keys S_{ID1}, S_{ID2}.

The following embodiments utilises identifier-based cryptography using Weil pairings to allow the generation of a public key that is a combination of independent identities associated with a set of n trust authorities (not shown). The trusted authorities can be totally independent to each other and there is no needs for any business relationship to exist between the trust authorities, in fact the trust authorities do not need to know each other.

The first embodiment utilizing Weil pairings allows the user to encrypt a document $m \in \{0,1\}^k$ for sending to the printer 30, which the printer 30 can decrypt if the printer 30 has a number of private keys S_{IDi} (i = 1, ..., n), each respectively issued by a trust authority TA_i (i = 1, ..., n) corresponding to a public key Q_{IDi} (i = 1, ..., n).

Each trust authority TA_i (i = 1, ..., n) respectively selects a random $s_i \in \mathbb{Z}^*_q$ and set $R_i = s_iP$.

The printer 30 registers with each respective trust authority providing each trust authority with an appropriate independent identifier, ID_i (i = 1, ..., n) $\in$ $\{0,1\}^*$.

Each trust authority then computes an appropriate MapToPoint ($H_1(ID_i)$) = Q_{IDi} $\in E/\mathbb{F}_p$ of order q and set the printer's corresponding private key S_{IDi} to be S_{IDi} = s_iQ_{IDi}.

To encrypt a document, m, the user 50:

Computes a MapToPoint ($H_1(ID_i)$) = Q_{IDi} (i = 1, ..., n) $\in E/\mathbb{F}_p$ of order q.

Selects a random number $\sigma \in \{0,1\}^k$.

Computes $r = H_3(\sigma, m)$, where r is a random element that ensures only someone with the appropriate private key can decrypt the document, m.

Computes $U = rP$.

Computes $g_{ID} = \Pi_{(1 \le i \le n)} \hat{e}(Q_{IDi}, R_i) \in \mathbb{F}_{p^2}$.

Computes $V = \sigma \oplus H_2(g_{ID}^r)$.

Computes $W = m \oplus H_4(\sigma)$.

Sets the ciphertext to be $C = (U, V, W)$.

To decrypt the message, m, the printer 30:

Tests $U \in E/\mathbb{F}_p$ of order q;

Computes $x = \hat{e}(\Sigma_{(1 \le i \le n)} S_{IDi}, U)$;

Computes $\sigma = V \oplus H_2(x)$;

Computes $m = W \oplus H_4(\sigma)$;

Computes $r = H_3(\sigma, m)$;

Checks $U = rP$.

By way of further illustration figure 3 shows a bookshop 300 that includes a printer 310; a first computer entity 320 associated with a book publisher 330 and also acts as a first trust authority 340; and a second computer entity 350 associated with the printer manufacture and also acts as a second trust authority 360, where the printer 310, first computer entity 320 and second computer entity 350 are connected via a network 370, for example the Internet.

The bookshop 300 allows customers to locally print books using the printer 310. For each book the book publishers 330 have provided the bookshop 300 with an encrypted version of the book encrypted using a public key derived using policies for two trust authorities 340, 360, as described above.

The first set of policies require that the second trust authority 360 (i.e. the printer manufacture) confirm the integrity and operability of the printer 310 before issuing an appropriate private key. The second set of policies, intended for the first trust authority 340 (i.e. the book publishers themselves), contains references to the book and the bookshop.

When a customer attempts to print a book the printer detects the two associated categories of policies and send the policies to the relevant trust authority 340, 360 to obtain the relevant private key required by the printer 310 to decrypt the book. Therefore, for a book to be printed off the book publisher 330 can be confident that the printer integrity has been checked by the printer manufacture and that the bookshop 300 has informed the book publisher 330 that the book has been printed, thereby allowing the book publisher 300 to charge the bookshop 300 for the printed book.

CLAIMS

1. A computer system comprising a first computer entity for deriving an encryption key using a first data set that defines at least one policy for allowing the printing of a second data set and encrypting the second data set with the encryption key; and communication means for providing the encrypted second data set to a printer; wherein a second computer entity is arranged, on satisfaction of the at least one policy, to generate an associated decryption key to allow the printer to decrypt the encrypted second data set.

2. A computer system comprising a first computer entity for deriving an encryption key using a first data set that defines at least one policy for allowing the printing of a second data set and encrypting the second data set with the encryption key; and communication means for providing the encrypted second data set to a printer; wherein a second computer entity is arranged, on satisfaction of the at least one policy, to issue an associated decryption key to allow the printer to decrypt the encrypted second data set.

3. A computer system according to claim 2, wherein the communication means provides the at least one policy to the second computer entity.

4. A computer system according to claim 2, wherein the second computer entity issues the at least one policy to the first computer entity.

5. A computer system according to any preceding claim, wherein the second computer entity is associated with a trusted authority.

6. A computer system according to claim 5, wherein the encryption key is derived with the first data set and a public parameter associated with the trusted authority.

7. A computer system according to any preceding claim, wherein the second data set is encrypted with the encryption key using a bilinear pairing or quadratic residue technique.

8. A computer system comprising a first computer entity arranged to generate an encryption key using a first data set that defines a first policy for allowing the printing of a fifth data set in conjunction with a second data set that represents a first trusted party's public key and a third data set that defines a second policy for allowing the printing of the fifth data set in conjunction with a fourth data set that represents a second trusted party's public key, and encrypting the fifth data set with the encryption key; and communication means for providing the encrypted fifth data set to a printer; wherein a second computer entity associated with the first trusted party is arranged, on satisfaction of the first policy, to issue an associated first decryption key and a third computer entity associated with the second trusted party is arranged, on satisfaction of the second policy, to issue an associated second decryption key, thereby allowing the printer to decrypt the encrypted fifth data set.

9. A computer system according to claim 8, wherein the communication means provides the first data set to the first computer entity and the third data set to the second computer entity.

10. A computer system according to claim 8 or 9, wherein the fifth data set is encrypted with the encryption key using a bilinear pairing.

11. A method for printing comprising deriving an encryption key using a first data set that defines at least one policy for allowing the printing of a second data set; encrypting the second data set with the encryption key; providing the encrypted second data set to a printer; arranging a first party to issue, on satisfaction of the at least one policy, an associated decryption key to allow decryption of the encrypted second data set, thereby allowing the printing of the second data set.

12. A method according to claim 11, further comprising providing the first data set to the first party.

13. A method according to claim 11 or 12, wherein the first party is a trusted authority.

14. A method according to claim 13, wherein the encryption key is derived with the first data set and a public parameter associated with the trusted authority.

15. A method for printing comprising generating a first data set that represents a first trusted party's public key; generating a second data set that represents a second trusted party's public key; generating an encryption key using a third data set that defines a first policy for allowing the printing of a fourth data set in conjunction with the first data set and a fifth data set that defines a second policy for allowing the printing of the fourth data set in conjunction with the second data set, and encrypting the fourth data set with the encryption key; and providing the encrypted fourth data set to a printer; providing an associated first decryption key to the printer generated by the first trusted party, on satisfaction of the first policy, and providing an associated second decryption key to the printer

generated by the second trusted party, on satisfaction of the second policy, to allow decryption of the encrypted fourth data set.

16. A method according to claim 15, further comprising providing the third data set to the first trusted party and the fifth data set to the second trusted party

17. A printer comprising a receiver arranged to receive a first data set encrypted using a second data set, wherein the second data set defines at least one policy for allowing the printing of the first data set.

18. A printer according to claim 13, wherein the receiver is arranged to receive an associated decryption key generated by a trusted authority on satisfaction of the at least one policy, thereby allowing printing of the first data set.

19. A printer according to claim 14, wherein the trusted authority is incorporated within the printer in the form of a computer entity.

20. A printer according to claims 11 or 12, further comprising a transmitter arranged to provide that at least one policy to a computer entity.

ABSTRACT

METHOD AND APPARATUS FOR PRINTING

A computer system comprising a first computer entity for deriving an encryption key using a first data set that defines at least one policy for allowing the printing of a second data set and encrypting the second data set with the encryption key; and communication means for providing the encrypted second data set to a printer; wherein a second computer entity is arranged, on satisfaction of the at least one policy, to issue an associated decryption key to allow the printer to decrypt the encrypted second data set.

Figure 1

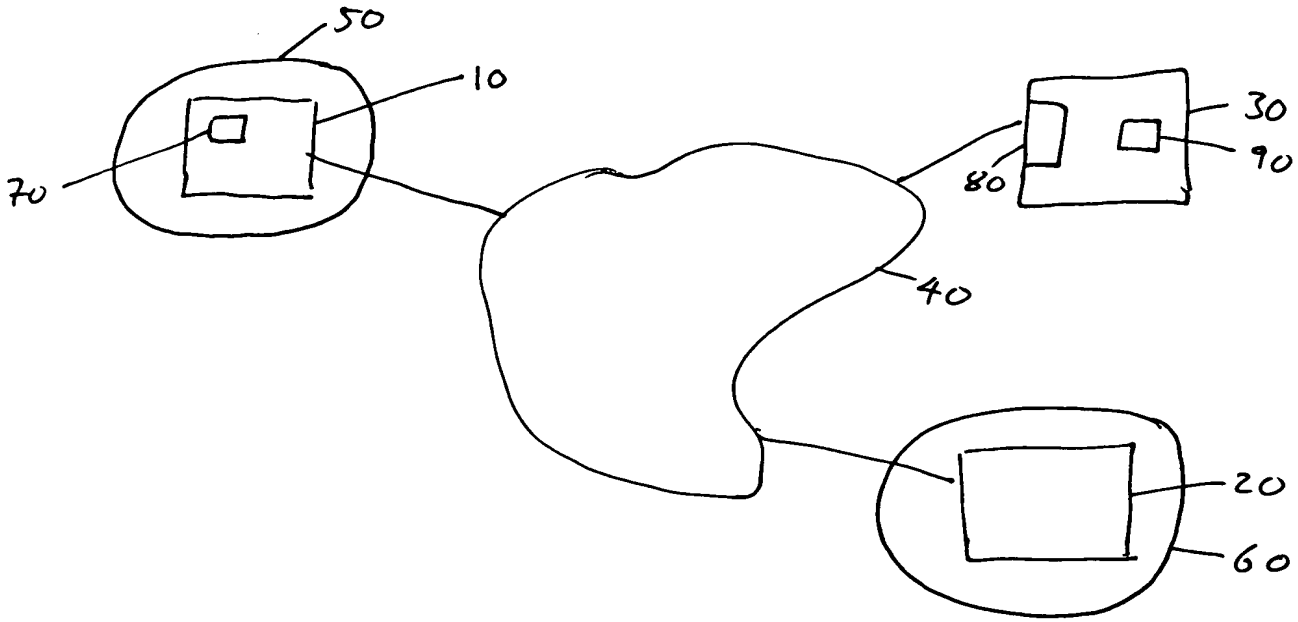

Figure 1

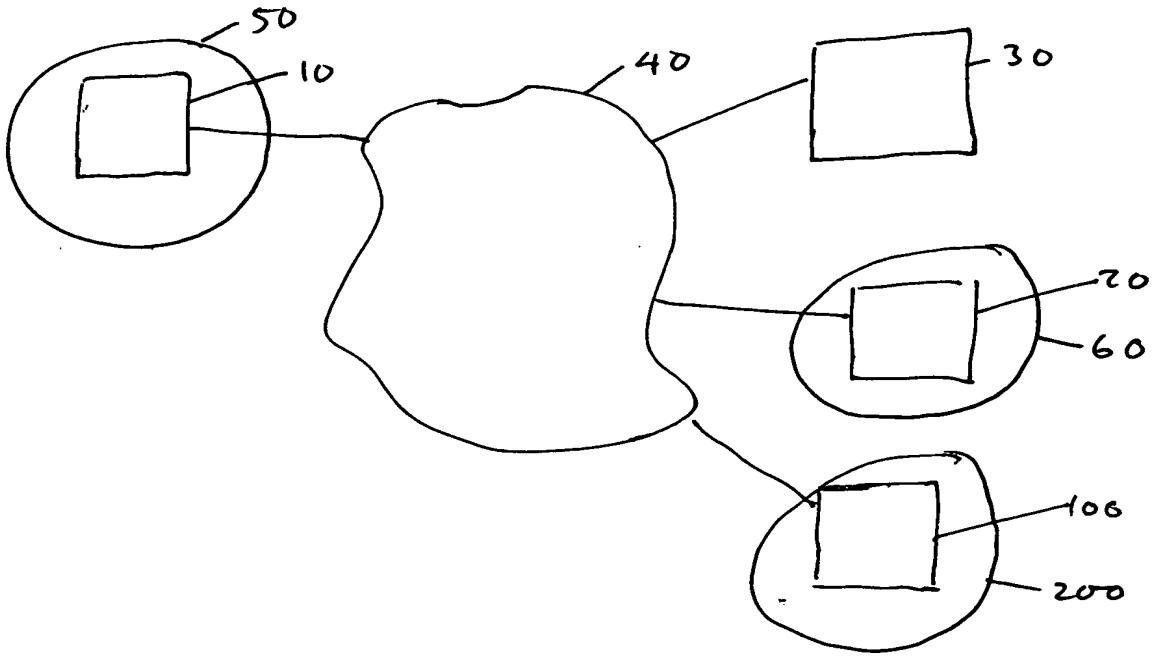

Figure 2

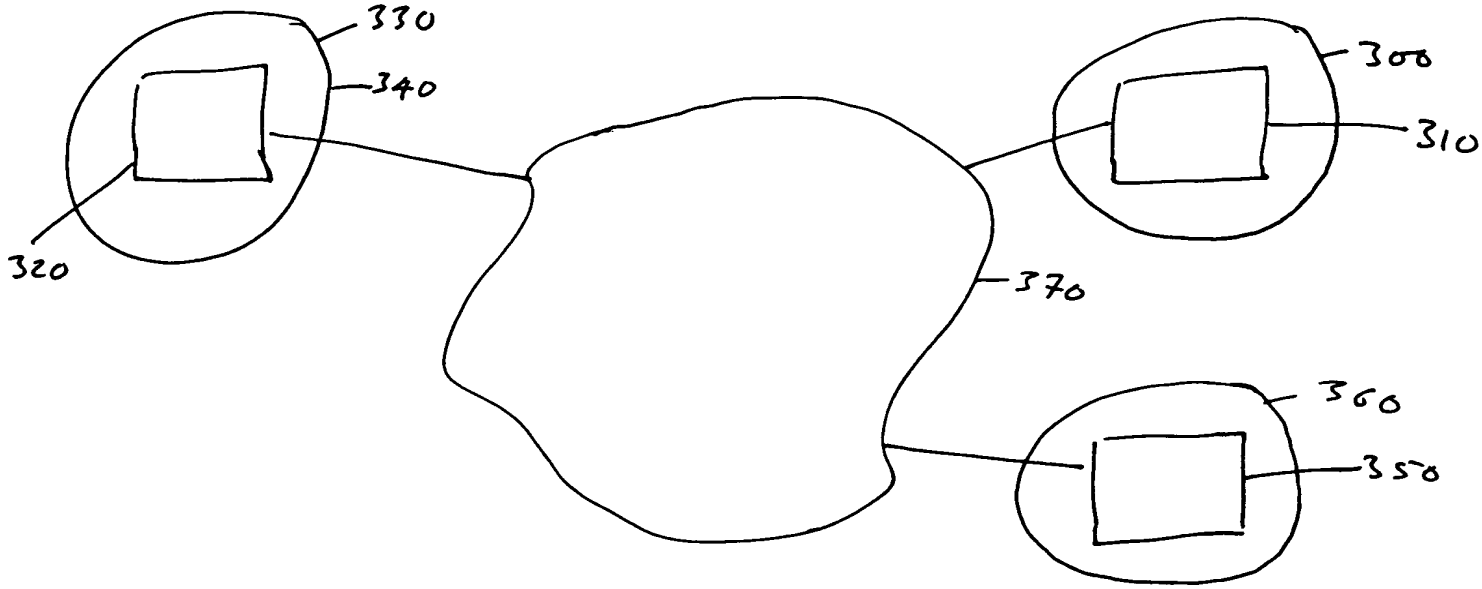

Figure 3